Striking the Balance between Privacy and Governance in the Age of Technology

Jing Ran

Introduction

In the past thirty years, information technology has in many different ways changed how we conduct our daily tasks and how our society functions. From individuals shopping and communicating with their friends online to the government monitoring epidemic outbreaks and tracking down criminals for security purposes, it has made both our lives and the government's jobs easier.[1] With the growth of technology, however, also comes with the concerns of individual privacy. While technology makes the state more powerful, proliferation of records and data has led to the decrease of protection over individual privacy.[2] Should and can we still maintain a balance between individuals and the state in the era of technology, and if yes, how should we do it? In this paper, I claim that privacy is still essential to our society as an individual, social and democratic value, and we need a balance between privacy and surveillance in the Information Age. As modern technology has rapidly grown out of existing legal framework and empowered states with more capability and information superiority, the balance has been shifted and unique challenges have been brought into the debate. To restore the balance – so as to protect individual rights and democratic values – requires a combination of legal, social and technological efforts.

In section one, I plan to examine the concept of surveillance and its role in facilitating governance. I will then move on to the other side of the argument – privacy – to examine the value of privacy and why we need a balance between it and surveillant governance. In section three, I will give a historical overview of how the balance between individual privacy and governance was challenged and maintained through the past century and what lessons we could learn from it. I will then examine what is so special about the Information Age, which parts of the privacy-surveillance debate has changed or not changed, and what unique challenges we face today to restore the balance. Lastly, I will present possible solutions to address each of the challenges and call for a combination of social, technological and legal initiatives to protect privacy.

Section One: The Role of Surveillance in Governance

Surveillance is helpful to governments in many ways: it allows them to gather more information and exercise more control, which is necessary for governments to fulfill their roles considering the increasing mobility and anonymity of modern society. However, unchecked surveillance that causes discrimination and inequality can also undermine a

1 Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York: New York University Press, 2004), 2.
2 Ibid.

democratic society.[3] What is the definition of surveillance, and how has it grown into a significant part of our social life? How might surveillance facilitate governance, and when is it considered undemocratic? This section attempts to address the above questions.

What is Surveillance?

Before discussing the more modern practices, it is necessary to examine some of the early theoretical framework on surveillance to better understand why the human society needs it and how it achieves its goals. Although activities of surveillance can be traced back to early stages of history, larger scale surveillance that we understand today, as an institutionally central and pervasive feature of social life, did not emerge until modern time.[4] Starting from social control in the workplace, surveillance is defined as a form of bureaucratic management that makes uses of knowledge and discipline by Max Weber, the best known figure of early analysis of surveillance.[5] This understanding of surveillance was later expanded to the broader context of society and governmental institutions by Michel Foucault's discussion of Bentham's Panopticon, a circular institutional design to observe and control prisoners with one single watchman in the center.[6] Foucault argues that surveillance system such as the Panopticon can create a self-policing apparatus to maintain social order with minimum governing effort. Today, the concept of surveillance becomes more sophisticated: as defined by Torin Monahan, a system of surveillance is one that "[enables] control of people through the identification, tracking, monitoring, and/or analysis of individuals, data, or systems".[7] However, early theories by Weber and Foucault still apply: surveillance, as a management system based on knowledge, will always strive for collecting more information in order to function better, and it still exists to serve the same role of imposing social control – which Monahan considers central to understanding surveillance – to "[order] society through the regulation of individual or group behavior".[8] These two important characteristics of surveillance remain true over time, and have even grown more prominent as the society becomes more modern.

The Rise of Surveillance in Modern Society

Why, then, was modern society facing a greater and greater need for such a system of institutionalized social control to manage business and governance? The answer comes from two aspects: the changing economic and the social structures.

In the economic aspect, capitalism has introduced new business practices in the

3 Kevin Haggerty and Minas Samatas, *Surveillance and Democracy* (Abingdon, Oxon: Routledge, 2010), 3.

4 David Lyon, *The Electronic Eye* (Minneapolis: University of Minnesota Press, 1994), 24.

5 Ibid., 25. ("In the capitalist workplace… [efficiency] is allegedly maximized through this system, but so is social control… rational administration is a fusion of knowledge and discipline.")

6 Michel Foucault, *Discipline and Punish: The Birth of the Prison* (New York: Pantheon Books, 1977), 195.

7 Torin Monahan, "Questioning Surveillance and Security," in *Surveillance and Democracy*, edited by Kevin D. Haggerty and Minas Samatas. Abingdon (Oxon: Routledge, 2010), 96.

8 Ibid.

work environment.[9] Based on Karl Marx's description of capitalism and Max Weber's notion of capitalist bureaucracy, David Lyon points out that modern surveillance originates from the emergence of large-scale business enterprises and their need to monitor and supervise their employees to enhance efficiency.[10] The new workplace relationship model caused many business owners to abandon previous administrative approaches no longer suitable for large-scale production and instead depend on the role of knowledge and well-measured information in generating and maintaining power in the workplace.[11] Surveillance came into place to serve the need of business administration required for capitalistic economy as an approach to manage at-scale workforce by collecting and maintaining relevant information.[12]

Surveillance has later grown into a more general governing technique in political arena as governments started to face similar needs of massive control due to increasing anonymity from urbanization and the growth of human society.[13] Before modern era, individuals mostly lived in small rural villages where familial bonds are usually shared and everyone knew and was known by everyone. (tense)[14] As human gatherings scales from towns to cities and even to countries, social order could no longer be maintained by previous bonds and tribal arrangement, because residents are now surrounded by strangers. With increased anonymity and mobility, massive surveillance by government institutions became necessary to guarantee security and order in modern society at a much larger scale.[15] As Haggerty and Ericson describes it, these practices mark "the progressive disappearance of disappearance," to make it difficult for individuals to remain anonymous or to escape social monitoring without losing their social benefits.[16]

How is Surveillance helpful in Governance?

After we have established that surveillance systems emerged in response to the increasing dependences on information for social control in modern society, we can see a simple reason why governments always push for maximizing surveillance and information gathering – more information makes their job easier from an administrative perspective. When properly used not against the society but to better serve it, surveillance means that government can fulfill their duty better with more information. After all, governments exist to collectively address real issues beyond individual levels such as negative externalities, public safety and regulations, and we want them to function well. One significant achievement of surveillance is public health surveillance efforts to control epidemic outbreaks. By tracking and monitoring clinical reports on spreading diseases, surveillance allows the government to take actions to prevent further harm of the society. Another perhaps more important function is to identify threats and maintain social order.

9 Lyon, *The Electronic Eye*, 27.
10 Ibid.
11 Ibid., 27.
12 Ibid.
13 Kevin D. Haggerty and Richard V. Ericson. "The Surveillant Assemblage," *British Journal of Sociology* 51, no.4 (2000): 219.
14 Ibid.
15 Ibid.
16 Ibid., 218

Surveillance practices such as CCTV cameras on the street and airport security screening allows law enforcement agency to function and to protect members of the society from criminal activities and other security concerns.[17] As Haggerty and Samatas argue, very few would claim that wire taps, informants, undercover work and other comparable practices should be abandoned all together, because they are required in today's police work against complex criminal organizations.[18] In this sense, some degrees of surveillance is a key component for a functioning liberal society to prosper. Although surveillance as a form of social control has usually been criticized as negatively associated with coercion and discrimination, proper surveillance is not only necessary but also inevitable to a well-functioning government.[19] In order to fulfill its duty of protecting national security, regulating illegal activities, and managing the population in a large scale, government needs to gather some information to make the correct decision and to administrate.

On the other hand, however, it should also be noted that surveillance can result in unfavorable situations where the administration abuses their power of surveillance to facilitate their own agenda. Throughout the twentieth century, surveillance has long been associated with totalitarian regime that controls every aspect of its society to maintain its ruling status, such as Eastern Germany's uses of secret police *Stasi* to gather information about any potential dissidents.[20] Even in the United States, the FBI has notoriously pushes its limits under J. Edgar Hoover to gather information at their discretion, which ended up in harassment of civil rights activists and politicians.[21] Surveillance could cause great problems without limits or oversights, and has to be exercised within certain standards.

Democratic vs. Undemocratic Surveillance

Since surveillance can enable the government to better serve the society when used properly, but harm individual rights when abused, it is important to evaluate what form of surveillance or social control is more democratic, and what standard should we use to decide it.

There are two ways of evaluating whether we consider a surveillance system democratic. The first and weaker one is whether the system is used for democratic ends: for example, surveillance by *Stasi* in East Germany and other totalitarian regimes is often used as abuse of power for personal agenda and thus clearly not democratic.[22] The second one is more concerned with the design and process of the system, even for a democratic government, such as surveillance programs set up by the National Security Agency (NSA) in the United States.[23] As Monahan proposes, we should evaluate a surveillance system based on whether it promotes democratic and egalitarian participation.[24] He claims that a system is democratic when it invites participation, facilitates learning, and achieves

17 Haggerty and Samatas, *Surveillance and Democracy*, 7.
18 Ibid.
19 Ibid.
20 Ibid., 5.
21 Simon Chesterman, *One Nation under Surveillance: A New Social Contract to Defend Freedom without Sacrificing Liberty* (Oxford: Oxford University Press, 2011), 232.
22 Haggerty and Samatas, *Surveillance and Democracy*, 5.
23 Monahan, "Questioning Surveillance and Security," 103.
24 Ibid.

some degrees of power equalization in local government or industry.[25] On the other hand, commonplace surveillance practices, though designed and exercised for democratic ends such as care or security, have few oversights and often result in coercion and repression.[26] This limitation of individual autonomy is against the principles of democratic governance, and such surveillance should be changed.

Section Two: The Value of Privacy

As the government pushes for more surveillance to facilitate its administration, on the other side of the debate, we also need to acknowledge that massive information gathering by the government contains great risks of compromising individual privacy and other democratic values when not regulated properly, even if it is useful in law enforcement and the maintenance of social order.[27] This section will first examine the concept of privacy, identifies privacy as a social value that should not be considered against to greater social good, and establishes privacy as a core value of democracy.

Conception of privacy

Privacy has been an important individual right and frequently referred to in everyday life, yet it is difficult to come up with an overarching definition of privacy that is neither too vague nor too narrow.[28] Each individual has different understandings of privacy, and it is even harder to apply various definitions into specific legal and political context. Many scholars and jurists have attempted to conceptualize the term and develop a theory of privacy.[29] Warren and Brandeis declared privacy to be "the right to be let alone" – a "general right to the immunity of the person, the right to one's personality."[30] E. L. Godkin, amongst others, proposed the limited-access theory on privacy as protection or control over the access to the self.[31] Some understand privacy as secrecy, and consider it violated when concealed information is disclosed to the public.[32] Others consider privacy a control over personal information, under which people can determine for themselves "when, how and to what extent information about them is communicated to others", thus defining privacy as a form of property.[33] Seeing such difficulty in defining the term, some theorists argue that privacy is just a derivative from other rights and thus reducible to them.[34]

Solove, on the other hand, argues that privacy has irreducible value in itself,

25 Ibid.
26 Ibid., 92.
27 Ibid.
28 Daniel J. Solove, *Understanding Privacy* (Cambridge, Mass.: Harvard University Press, 2008), 12.
29 Solove discusses several theories of privacy including the right to be left alone, limited access to self, secrecy, control over personal information, personhood, and intimacy. See Chapter 2 "Theories of Privacy and Their Shortcomings" in Solove, *Understanding Privacy*.
30 Ibid., 15.
31 Ibid., 19.
32 Ibid., 21.
33 Ibid., 25.
34 Ibid., 37. (Here Solove discusses the reductionists such as Judith Thomson, yet considers privacy issues far too multifarious to be reduced to rights over the person and property.)

yet there is no one core element that constitutes privacy, so the current attempts for a unifying definition must be replaced by a more pluralistic conception.[35] Privacy should be regarded as an umbrella term that consists of many different, interconnected elements, in order that legal framework and protection around it will function in a meaningful way to solve the real problems. The ambiguity of the concept of privacy has been central to many ongoing debates between privacy and governance. When governance often has tangible claims and benefits regarding security and social order, the value of privacy can be easily overlooked when it is defined as something insignificant or negative. One such argument is that one has nothing to hide if one has done nothing wrong, framing the claim of privacy as an excuse to hide wrongs. Solove addressed this argument by pointing out that privacy is not about hiding something bad and this understanding of privacy as a form of secrecy is myopic.[36] People's fear of violation of privacy is not so much about their inhibited behavior, but more a sense of powerlessness and vulnerability when facing the information superiority of the government who can make decision that will significantly impact your life based on your possibly distorted or oversimplified personal data. Another such argument contrasts privacy, a vague concept with no directly impactful values, with the greater good of the society, yet this argument has mistakenly contrasted privacy with social values, as illustrated in the next few paragraphs.

Privacy as a social value

When arguing in favor of privacy, many took the approach of rejecting the totalitarian model that places societal good over individual rights, but inevitably still falling in the mindset that there is a constant tradeoff between privacy and social good.[37] As an individual right, privacy is traditionally considered as merely valuable to individuals, and thus often compromised when in tension with the greater good of the society during war or more generally time of insecurity. Taking a step back, I argue that protecting privacy does not necessarily mean we are compromising the benefit of the larger society. As each individual values privacy as a fundamental right and can only live and work well with privacy protection, the same individual, as a social being, can only contribute to the welfare of a society through production and social engagement when feel safe about their privacy.[38] In this sense, privacy is also constitutive of society.[39] The tradeoff mindset that views privacy individualistically makes privacy undervalued, and protection based on such understanding will be insufficient to make up for the real harm caused to the victims of privacy violation. The interests privacy needs to stand up against – such as security, free speech, efficiency and economic development – are often framed in terms of social values, so if claims to protect privacy are limited on the individual level, they do not have much philosophical ground in the debate. One example is the Patriot Act after the attack

35 Ibid., 45.

36 Daniel J. Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security* (New Haven, Conn.: Yale University Press, 2011), 27.

37 Solove listed and criticized traditional liberalism that views privacy as a right possessed by individuals and intension with the larger community held by Richard Hixson, Thomas Emerson, and Warren and Brandeis. See Solove *Understanding Privacy*, 89.

38 Ibid., 91-92

39 Ibid.

on September 11, 2001, that enlarges the scope of information sharing for intelligence purposes.[40] The Patriot Act was passed in an overwhelming panic over national security in which arguments for individual privacy were easily ignored when facing security issues involving the society as a whole, yet later became highly controversial when its implication to privacy protection became clearer.[41] As Solove argues, if privacy is always understood as the opposite of greater societal good, it is hard for individuals to claim that their needs for privacy trump the welfare of an entire society.[42]

However, privacy indeed promotes the communities we live in and protects individuals from harm and disruptions to important social activities as well. It has a profound impact on the power structure of society and freedom each member has. In a more pragmatic model, privacy is valuable based on its contributions to society.[43] The harm of losing privacy on public life, creative processes, culture and freedom of speech should all be taken into account when evaluating privacy and how much social benefits it can bring.[44] To take a step further, privacy, as a protection of individual liberty and independence, is essential to a democratic society.

Privacy as Protection of Liberty and Core Value of Democracy

The value of privacy as to democratic society has been widely discussed by various political philosophers. As mentioned earlier, Foucault's analysis of the Panopticon system shows how the deprivation of privacy under massive surveillance that imposes power and discipline to individuals who are being watched leads to self-censorship and obedience.[45] In his theoretical discussion of privacy and democracy, Joshua Cohen regards privacy as central to democratic participation because of its protection independence of judgment. [46] Privacy rights, he argues, is essential in creating and maintaining a society of equals and its pluralistic philosophies, and thus should be understood as expressing democracy's core value, as opposed to constraining such expression.[47] Surveillance practices such as FBI's monitoring of activists and politicians under Hoover, as a real life example, greatly discourages political participation by imposing discrimination against the principle of equality. As John Dewey argued, that democracy is "more than a form of government," but also a mode of living based on social equality, long lines of race, gender, and other categories of differences.[48] In a society without privacy protection, social equality that precedes democracy will no longer be in place.

Thus, if we accept that privacy rights are the basis for personal liberties, and

40 Solove, *Nothing to Hide*, 76.
41 Ibid., 155-157.
42 Solove, *Understanding Privacy*, 93.
43 Ibid., 91.
44 Ibid.
45 Foucault, *Discipline and Punish,* 196.
46 Joshua Cohen, "Privacy, Pluralism and Democracy," in *Philosophy, Politics, Democracy: Selected Essays* (Cambridge, Massachusetts: Harvard University Press, 2009), 305.
47 Ibid.
48 John Dewey, *Democracy and Education* (Champaign, Ill.: Project Gutenberg, 1916), 101.

personal liberties are constitutive in public reason in the democratic process, we should understand why privacy rights are essential to democracy. Privacy protects two types of interests: those that avoid disclosure of personal matters and those in making independent judgment on important issues without interference.[49] Both interests are necessary in democratic deliberation and civic dialogue.[50] Poor privacy standards in cyberspace, as claimed by Paul Schwartz, will not only discourage participation in deliberative democracy but also undercut the development of individual capacity for self-governance.[51] If equal participation, independent judgment and social equality in governance process are required for democratic society, then privacy rights should be in place to protect these values.

Section Three: Historical Balancing between Privacy and Governance

Now that we have examined arguments on both sides of privacy and governance, we see that to have both a well-functioning government and a democratic society protected under privacy rights, there is a subtle balance between privacy and governance. Public policy debates and initiatives in the United States over the past century have shifted the balance back and forth: the government always pushes for more information through surveillance, while privacy rights activists fight back to protect against a totalitarian style of governance. In this section, I will present a historical overview of institutions and legal frameworks set up by the administrative, judiciary and legislative branches in response to historical events and technological development.

Hoover's FBI, Katz v. US, and Church Committee

Since governance and law enforcement are easier with information superiority over the population,[52] privacy could be easily compromised without legal protection when governmental agencies pushed for greater surveillance and more information during the time of need. As Fourth Amendment was considered inapplicable to wiretapping at the time according to *Olmstead v. United States*, and statutes inhibiting wiretapping was largely ineffective, surveillance through wiretapping was widely used during World War II and the Cold War for intelligence purposes.[53] As mentioned earlier, FBI under Hoover bugged and tapped not only potential threats to national security, but also dissidents, justices, professors, writers and scientists.[54] The balance between privacy and governance was broken, with the government abusing their power of surveillance for excessive control and personal agenda.

Fortunately, fights to restore the balance come from all three branches of government in the next few decades. *Katz v. United States* in 1967 overruled *Olmstead* and

49 Cohen, "Privacy Pluralism and Democracy," 311.

50 Ibid.

51 Paul Schwartz, "Privacy and Democracy in Cyberspace," *Vanderbilt Law Review* 52 (1999): 1613.

52 See discussion on surveillance and Max Weber in Section One.

53 Jeffrey Vagle, "Furtive Encryption: Power, Trust, and the Constitutional Cost of Collective Surveillance," *Indiana Law Journal* 90 (2015): 124.

54 Solove, *Nothing to hide*, 7.

established the "reasonable expectation test" for the scope of Fourth Amendment protection, laying the groundwork for further legislation to regulate electronic surveillance.[55] After Nixon's abuses of surveillance during Watergate Scandal, Congress also realized the need to examine government agencies and thus dedicated an eleven-member special committee led by Senator Frank Church on the issue of surveillance. Known as the Church Committee, this committee showed with fourteen volumes of reports and supporting documents that the abuses of surveillance conducted by the government has been excessive.[56] In response to reports published by Church Committee, Attorney General also regulated FBI investigations with a set of guidelines, and the FBI itself underwent major reforms to avoid further abuses of power.[57] Although increased surveillance granted the government more power for a few decades, it later received hostile responses from the population, and the respect of privacy was restored. However, this balance was soon challenged again by the growing technology.

Stored Communication Act (1986)

As technology advanced, earlier legal principles that protected individual privacy can no longer provide adequate guidance due to its vagueness and inapplicability to the new context. Under such circumstances, Stored Communication Act of 1986 was introduced to restore the guidance on privacy protection. *Katz v. United States* has established that Fourth Amendment should protect individuals' rights when the government violates their reasonable expectation of privacy, yet the test has become more ambiguous in the context of new technologies such as emailing, and the protection from the constitution is much weaker when applied to online information held by a third party.[58] To address such issues, the Stored Communications Act (SCA) came into place to provide privacy protection for stored wire and electronic communications held by third party internet service providers such as emails.[59] Under the SCA, the government has limited power to require internet service providers to reveal metadata on information not related to content, thus protecting privacy of the owners of these data.[60] The SCA was a great example of how legal framework for privacy protection should evolve accordingly with new technology, yet also later shows how fast it could become outdated.

CALEA (1994 – expansion in 2004)

While efforts to restore privacy protection moved forward, the government also tried to push for more convenience to obtain information from third parties by enacting policies favoring the surveillance side of the debate. In 1994, the Communication Assistance for Law Enforcement Act (CALEA) was passed to force telephone companies to redesign their network architectures to ease law enforcement's need of wiretapping digital telephone

55 Vagle, "Furtive Encryption," 125.
56 Solove, *Nothing to Hide*, 10.
57 Ibid.
58 Orin S. Kerr, "A User's Guide to the Stored Communication Act - and a Legislator's Guide to Amend It," *George Washington Law Review,* 72 (2004): 2-3.
59 Ibid.
60 Ibid.

calls.[61] The act was originally adopted based on FBI's concern that it would be impossible to conduct any surveillance with an upgraded design of phone switches, but was expanded to cover internet service providers and communication services like Skype in 2005.[62] A few years later, FBI is pushing to expand CALEA to all online communications software, as part of many efforts that law enforcement agencies try to control more online data.

Today, new computer technology seems to have created a new arena between privacy and governance; fights to maintain the balance between privacy and governance have only intensified.[63]

Section Four: Break of Balance in Information Age

The tension between privacy and surveillance is nothing new, yet under today's new technology and the government's cooperation with large players in the private sector, state surveillance has become immune to some of the traditional limits. Have the styles of governance that we rejected still living in the same way, in the same form, but just less explicit through the use of technology? This section aims to answer these questions by examining which parts of the debate have not changed in today's context, while which ones have. I will then further argue that the changed parts of the debate have tipped off the balance favorably towards the government side and posed unique challenges that need to be addressed with new solutions.

Parts of the Debate that have not Changed

In the public discourse on privacy and surveillance nowadays, we can still hear a lot of familiar arguments such as "you have nothing to hide in your email if you did not do anything wrong," "there is no point of caring about privacy on the internet," or "law enforcement needs to collect all the traffic in order to catch cyber thieves." Although the context of these arguments changed from CCTV camera recording and wiretapping to the internet and computers, they are intrinsically the same as the old arguments and can thus be easily addressed by the framework of privacy rights established before.[64]

There are three parts of the debate that have not changed. The first is the question on the value of privacy. Although it has been increasingly difficult for individuals to protect their privacy as they rely more on third-party technology to store, send and receive personal data, it does not mean that they no longer care about the control over these data. No matter how the platform on which potential privacy violation occurs has changed, privacy still shares the same philosophical values both on individual and social levels.[65] Privacy rights still promote values liberty and independence of judgment that are essential to democratic society, and, prescriptively speaking, should thus be cared about and protected even on the internet.

61 Electronic Frontier Foundation, "CALEA," https://www.eff.org/issues/calea.
62 Ibid.
63 Ibid.
64 See discussion on the value of privacy in Section Two.
65 Ibid.

The second is the function of surveillance and its role in governance. In order to fulfill their duty, governments need data to govern the modern society and combat sophisticated criminal networks at large scale, and some degrees of surveillance is necessary.[66] Surveillance serves the same function of making administration easier, not matter by using paroling, wiretapping, security cameras, or big data analysis.[67] As Lessig argues, liberty online will not come from the absence of state, but a state of a certain kind, as anywhere else.[68] Data collection to catch cyber criminals, serving the same roles in governance as search and seize to find thieves, should thus be authorized under the same amount of scrutiny, not bypassing existing legal principles as an exception.

The last one is whether privacy and security is an all-or-nothing tradeoff. Solove argued against the all-or-nothing fallacy by showing that we are not making a choice between security and nothing, but between security with oversight and regulation and security at the sole discretion of governmental officials.[69] In this sense, the privacy-security debate in the context of the internet still needs to maintain a balance as before, and this should be the aim of public policy design.

The unchanged parts of the debate, which primarily deal with prescriptive grounds, could be addressed by the same theoretical framework we established earlier.[70] There still are values to both privacy rights and appropriate surveillance, and a balance can and should be struck and maintained between them.[71] Other parts of the debate have nevertheless changed in the new context and thus are more challenging to respond to.

Parts of the Debate that have Changed

What is more challenging, however, is the part of the debate that has indeed changed in the Information Age and thus presents new challenges that could not be addressed by the traditional theoretical discussion on privacy. There are mainly five issues about surveillance practices over computer technology that need to be examined specifically.

The first one is people's expectation of and general social norm of privacy on the internet. Although the conception of privacy has always been diverse, it was easier to reach a consensus before as people have physical control over their private information. The social norm was relatively clear that people should have privacy rights to prevent others from entering into their house or reading their letters, at least not with a warrant or other probable cause, if they do not wish so, and such expectation of privacy was more commonly shared and less ambiguous. Today, however, with information recorded and transmitted, and data centers and mail transfer servers located far beyond our reach, it is

66 See discussion on how surveillance is helpful to governance in Section One.
67 Ibid.
68 Lawrence Lessig, *Code*. Version 2.0. (New York: Basic Books, 2008), 4.
69 Solove, *Nothing to Hide*, 37.
70 See discussion on the benefits and issues of surveillance in Section One and privacy in Section Two.
71 Ibid.

more difficult for us to reach a clear consensus on what we expect to be private.[72] As Paul Schwartz puts it, there is an absence of appropriate and enforceable privacy norms that prevent traditional privacy law to effectively function in cases regarding modern computer technology.[73]

The second one is decreased transparency and reduced participation caused by surveillance technology. As Justice Sotomayor points out, one natural limitation of conventional surveillance is the community hostility when they notice increased policing activities.[74] Before, surveillance are usually visible to those who are watched, which will result in more awareness and advocacies to maintain the balance if it moves too much towards governance from individual rights, thus incorporating public participation into the system. New technologies, however, are often designed with an exclusionary nature and less visible to the community, thus reducing the previous check on surveillance from the community.[75] Analysts in law enforcement office today can process data they collected from security camera or online traffic without paroling on the street and being seen by members of society. To make it worse, opaque algorithms make it more difficult for individuals to know what data have been saved, gathered and sent when they interact with computer software or mobile apps and thus unaware of the potential privacy implications.

The third challenge, similarly, is the elimination of man power limits that gives government larger capability. In the same court opinion, Justice Sotomayor argues that modern surveillance technology has also reduced the traditional limits of costs and man power.[76] She used the example of GPS monitoring the track down a person's movement, which has much lower cost compared to conventional techniques that use extensive man power, and has thus evades the checks that constrain abusive law enforcement practices.[77] One other example is use of license plate reader by the NSA to track down automobile movements, which allows the computer to process and classify information much faster than having policemen following each car on the street. In both cases, the government can now use limited police resources to gather a substantial quantum of intimate information, and this, as Sotomayor argues, may "alter the relationship between citizen and government in a way that is inimical to democratic society."[78]

Fourthly, the legal framework governing surveillance has long been outdated and easily outpaced by the fast growing technology. As past regulations that constrains government's power only covers existing technology at the time, cases based on new technology has to rely on updated legislation or is open to judiciary interpretation. As shown in the last section, Stored Communication Act of 1986 attempts to offer Fourth-

72 Schwartz, "Privacy and Democracy in Cyberspace," 1611.

73 Ibid.

74 United States v. Jones, 565 U.S. 10-1259 (2012) (Sotomayor, J., concurring). ("The Government can store such records and efficiently mine them for information years into the future… because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: limited police resources and community hostility.")

75 Monahan, "Questioning Surveillance and Security," 92.

76 See note 74.

77 Ibid.

78 Ibid.

Amendment-like privacy protection for digital communications stored online and has been effective for some periods of time, yet soon fails to accommodate new service model on the internet.[79] As SCA differentiates between electronic communications server – unopened email within 180 days – and remote computing service – emails over 180 days and stored purely for the purpose of providing storage or computer processing services, it only requires a search warrant for the former, while a much lower requirement is applied to the latter.[80] This means SCA cannot provide as much protection as we would hope today, when most emails are stored on the server and cloud computing has become a new lifestyle. The lack of legislative progress on internet privacy since SCA has been highly incompatible with the acceleration of the technology industry, yet further shows the issue of outdated legal framework in the debate.

Lastly, we rely much more on third party private enterprises, and surveillance involves increasing public and private collaboration. As people spend more and more of their interaction and social life via third party platforms – websites, mobile phones, etc – government starts to collect data and conduct surveillance with close collaboration with private enterprises.[81] As Lessig argues, in the age of the internet, the government's power comes not just from chips but from a government-commerce alliance.[82] As commerce fares better with a well-regulated society, it will supply government with the resources to build up stronger regulation and control, through direct and indirect means.[83] What protection do we then have, when our private information is stored and controlled by third party actors who might turn over our data to the government? Far fewer than what we used to have.

Break of Balance by the New Challenges

With technological advancement and its unique characteristics, the internet and new surveillance techniques have tipped the balance between privacy and governance favorably towards the government side. Although technology becomes a more important part in human interaction in everyday life and individuals have become more connected, the understanding of privacy protection seems to still lag in the past tense. The approach of assuming no privacy expectation when information is disclosed to a third party, as Justice Sotomayor argues, is ill suited to the digital age, where mundane tasks like dialing to the cellular providers, visiting URLs and purchasing groceries and medications online are all carried out through third parties.[84] It is now much more difficult to reach a consensus on

79 See discussion on *Stored Communication Act* in Section Three.

80 Kerr, "A User's Guide to Stored Communication Act," 4.

81 Lessig, *Code*, xiii.

82 Ibid.

83 Ibid.

84 United States v. Jones, 565 U.S. 10-1259 (2012) (Sotomayor, J., concurring). "More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties… This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year."

the reasonable expectation of privacy, which results in a significant weakening of Fourth Amendment and the lack of other legal framework to protect privacy.[85] Dependence on third party private enterprises in social interaction and the lack of legal protection for such interactions have made individuals more vulnerable under surveillance practices by the government in collaboration with the private sector. While protections of individuals become weaker, the government, on the other hand, has become strong as empowered by technology.[86] Throughout the past century, the government has expanded its governance techniques to protect security. In the past, law enforcement relies mostly on searching houses, people and documents, while now they have more tools for information gathering from collecting records and data, conducting audio and visual surveillance, tracking movement and other big data analysis.[87] Conventional constrains, such as community hostility and policing resources, have diminished as new technology makes aggregation of information cheaper and less transparent. Information superiority has made the government more powerful, while leaving the individuals few tools to counterbalance the power structure. These special aspects of computer technology has broken the balance between individuals and the government, and must be addressed with new responses.

Section Five: Responses to New Challenges to Restore the Balance

The balance between privacy and governance needs to be restored and maintained, yet the new technological environment has imposed new challenges. This section propose potential solutions to each of the unique challenges from last section under the context of fast growing technology. I would like to claim that in order to maintain strong privacy protection against abuse of power and unreasonable surveillance, we need a combination of public campaigns, legal reforms and institutions, and technological designs that are more democratic with contributions from private companies.

The first challenge we are facing is the diverging conception of online privacy. A big problem that needs to be addressed is simply that there have been enough discussions and awareness by the general public. A large part of the population have never considered whether their expectation of privacy online matches up with how much privacy they actually have under current government surveillance, and are thus missed out in this debate of understanding privacy. While some might consider that there is a tradeoff of privacy for convenience and thinks it is inevitable to expect no privacy on the internet, it is unlikely that most people would simply give up legal protection and accept warrantless disclosure to the government of their browsing history.[88] One solution, therefore, is to increase public awareness of what we should reasonably expect for our online behavior as an individual who values privacy, and stand up to fight against incidents when such expected privacy is violated. It is much easier to make progress in bridging this diversion when we have more people joining the conversation and contributing to the debate.

The second challenge is the decreased transparency because surveillance technology now requires more technical knowledge to understand and thus less

85 Solove, *Nothing to Hide,* 114.
86 Ibid., 102.
87 Solove, *Nothing to Hide,* 12.
88 See note 84.

straightforward to allow public participation. One solution to this is better media coverage of technology and increased technical education. When the general public is more educated about what implications each surveillance technology has, they can make more informed decision and observation on what the government can do. For example, an individual might not have understood what NSA's license plate reader can do, but after reading an article that specifies how this technology allows NSA to track the movement of each automobile owner, there will be more public discussion on whether the use of such technology is appropriate. Similarly, better technical education can allow individuals to understand how one software product leaves less room for government surveillance than another, and thus make informed decision on which one to purchase. Admittedly, this solution might not be practical to implement, but does provide a possibility of restoring the balance. Another solution is Monahan and Lessig's call for democratic surveillance as incorporated in the design of technology.[89] Certain technological design will make it harder for the government to install a backdoor without harming the overall security of the technology, therefore preventing undemocratic abuse of power on the design level.[90] Although the public is usually excluded from participation in technical issues like telephone line design and communication network, there are ways to make the use of a technology more transparent and thus encourage public supervision.[91]

The third challenge is the diminishing limit of surveillance man power. New technology has made massive surveillance cheaper, therefore granting the government more power to collect information with little additional cost. The solution I want to propose here, however, is not a technical one but a political or legal one. It is true that computer technology has transformed a lot of ways how government gather information, yet there are few ways to force technology to go backward in time. Technology will keep advancing through different generations, but it is ultimate just a tool and depends on how people are allowed to use it. What really matters is not how efficient technologies are, but whether they are used with regulations and oversights.

Consider computers as another form of man power. It would have made *Stasi* in East Germany and Hoover's FBI more powerful, but what these agencies did, no matter using man power or technology, should not have been allowed in the first place. What is at stake here is whether governmental agencies should be allowed to massively collect data, not how efficient they did it. For example, wiretapping has also greatly reduced man power required for surveillance when it first emerged, but once there is oversight from Congress by the Church Committee, the use of it can be regulated with proper administrative guideline and legal framework.[92] I argue that computer technology is merely a more advanced version of electronic surveillance, and thus the solution is to regulate it with oversight under an established political and legal framework, which leads us to our fourth challenge.

The fourth problem to address is the soon-outdated legal framework compared to the fast-growing technologies. One problem with most past technology regulations and statutes that refrain governmental power is that they only protect privacy rights in specific ways of social interaction and were built closely with existing technology at the time when

89 Lessig, *Code,* 6 and Monahan, "Questioning Surveillance and Security," 93.
90 Lessig, *Code,* 6.
91 Monahan, "Questioning Surveillance and Security," 93.
92 Solove, *Nothing to Hide,* 10.

they were passed, without enough flexibility to accommodate technological evolution. Therefore, as new technology emerges, the decision of whether the new issue still falls under the old framework is passed to courts, and an updated version of the regulations is generally needed for the emerging technology. For example, when telephone and early POP-protocoled email first became popular in society, it soon became clear that existing legal frameworks were insufficient to regulate surveillance over these technologies, so CALEA and SCA were established respectively in response to each technological advancement. However, as cloud computing and email storage enters into the mainstream, SCA has also become outdated in regulating remote computing services, and new legislative and judiciary efforts become necessary.[93]

It is worth noting that the fact that outdated legal framework has not been effective in protecting privacy does not mean we should give up on legal protections all together. Particularly, some who are disappointed at protection of privacy by the current legal system took the approach of Crypto-Anarchy – a belief that strong cryptography to keep all their online communication encrypted from the government is the best way to protect their privacy and political freedom.[94] This approach can successfully ensure privacy, but will also abandon any role we want the government to fulfill. Referring to the earlier section on the role of surveillance and governance, there is a reason why governments exist and there are duties we want them to fulfill with certain technology, including regulating the cyberspace.[95] The law that governs cyberspace might be outdated and ineffective, but is still necessary and beneficial.

How, then, can we ensure that legal reforms can catch up with the speed of technological advancement? One lesson to learn from SCA is that the law needs to be designed with more flexibility while jointly considering how legislative and judiciary efforts interact.[96] As Solove argues, this problem of technology and law cannot be solved by one-sidedly favoring legislatures over courts or vice versa.[97] On the legislature side, we need to have laws that are sufficiently broad and flexible to accommodate the rapid speed of technological growth. However, such breadth and flexibility must be carefully interpreted on the judiciary side to avoid vagueness and to be enforceable as intended.[98] Internet privacy scholars have suggested different principles for the framework to regulate evolving technology. Solove for one argues that we should regulate information gathering by the government when it causes "problems of reasonable significance", and proposed three principles: minimization of data gathering and use and deletion after a reasonable period of time, gathering under particularized suspicions, and proper oversight.[99]

The last challenge is the increasing dependence on third party and the collaboration between government and commerce in the Information Age. While legal reforms as mentioned in the last few paragraphs can for sure refrain government from requesting

93 Kerr, "A User's Guide to Stored Communication Act," 20.

94 Steven Levy, *Crypto: How the Code Rebels Beat the Government, Saving Privacy in the Digital Age* (New York: Viking, 2001), 196.

95 See discussion on the role of surveillance in Section One.

96 Solove, Nothing to Hide, 122.

97 Ibid., 171.

98 Ibid.

99 Ibid.

customer data from or installing a backdoor at private enterprises, to restore the balance and protect privacy rights, we have to go beyond the laws to social norms and even to computer code itself.

In his book *Order Without Law*, Robert Ellickson discusses how people more often apply informal societal norms than formal legal rules in resolving disputes.[100] A society's operative norms that involves enforcement activity – such as rewards and punishments – exercises stronger social control on the population[101]. This theory presents a pragmatic approach of promoting privacy through norms: if privacy protection in new technology becomes part of the expected social norms, companies are bound to include it not because of legal requirements but because corresponding rewards and punishments will be enforced on them by the society and the market. For example, companies failing to protect privacy will lead to the punishment of the loss of customers and hostility from the technology community as imposed by the society. In the meanwhile, companies that do value privacy will have a competitive advantage in the market, and such practices will therefore be further promoted. In this sense, the protection of privacy can be better addressed not by formal laws but by social norms that bind the technology industry.

Furthermore, these norms are also implemented deeply into the technology itself. As Lessig argues, cyberspace requires a broader term of "regulation", beyond the traditional lawyer's scope, by computer code.[102] Code decides how and what digital objects and information can be accessed by whom, and we can make design decisions to regulate cyberspace while we build software and architecture in it.[103] It is true that although the application of technology is often seen as political, its design is traditionally considered apolitical and motivated by the free-market.[104] However, technological design has a significant role in political pursuit of privacy and liberty as well.[105] As Neil Richards points out, how much privacy and civil liberties we have today depend largely on business and engineering decisions by those companies who made the software. In order for the society to exercise civil liberties and protect their privacy, we need to have technologists and engineers who value free speech and intellectual privacy as part of their professional ethics and build them into the system in their design.[106] Monahan considers the current popularity of open-source software as an opportunity to move in the direction of democratization of technology, yet more broadly speaking, technologies as intermediates like ISP, email provider, telephone network and social media sites are the institutions through which we

100 Robert C. Ellickson, *Order Without Law: How Neighbours Settle Disputes* (Cambridge: Harvard University Press, 1991), 122.

101 Ellickson understands social norms from a very utilitarian perspective. When explaining why social norms were created, he relied on repeated game theory and argued that developing and maintaining these social norms can maximize the aggregated welfare that members of the society can obtain from the public affairs with each other. See Ellickson, *Order Without Law*, 128.

102 Lessig, *Code*, 5-6.

103 Ibid.

104 Neil Richards, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (New York: Oxford University Press, 2015), 169.

105 Ibid.

106 Ibid., 170

speak, and their incorporation of democratic architectures can have a huge impact on public participation.[107] The fight to restore the balance is not only for users and activists, but also substantially for technology companies. A solution to the challenges presented by the Information Age should include not only legal code – the East Coast code – but also computer code – the West Coast code.

Conclusion

As modern technology develops rapidly and becomes a more important aspect of society, it has also created an imbalance between privacy and governance by empowering states with information superiority while weakening traditional protection of individual privacy. The balance between privacy and surveillance has been heavily debated over the past century with a lot of public policy initiatives and legal proposals. There are merits to both sides of the argument: on one hand, institutionalized surveillance, as a theoretical concept of control widely discussed in contemporary political philosophy and closely associated with arrangements of modern and capitalist social structure, facilitates governance and is necessary for a well-functioning government; on the other, privacy rights, though hard to define with a unifying notion, has a lot of individual and social values and must be protected against abuse of power to ensure independent judgment and equality essential to a democratic society. In the past few decades, privacy protections have been constantly challenged by the government's push for more information and control such as wiretapping and other intelligence practices under Hoover, but a series of legislative, judiciary and administrative efforts such as SCA, *Katz v. United States,* and guideline of FBI by the Attorney general were also passed to strike the balance.

Entering into the Information Age, some parts – the value of privacy, function of surveillance and how significant is the tradeoff – of the debate between privacy and surveillance remain unchanged, while others are fundamentally altered by the new computer technology. What is a reasonable expectation of privacy online becomes more ambiguous; efficient and cheap surveillance techniques has caused the traditional limits of man power and community hostility on overboard surveillance to diminish, thus reducing the checks on government power; legal frameworks are too outpaced by the speed of technological growth to provide the protections as before; reliance on third party in everyday life and collaboration between government and these third parties have made individuals more vulnerable to surveillance.

These new challenges must be addressed with new solutions. Raising public awareness on the state of privacy on the internet will encourage more conversations to form a new social norm, and increasing media coverage and technical education will also make the population more informed on technological surveillance and how to protect their privacy. Moreover, a more flexible legal framework that can accommodate evolving technology while remains enforceable requires efforts from both the legislatures and courts. Lastly and most importantly, we have to look beyond laws to societal norms – beyond legal code to technical code – for a more democratic cyberspace, as a large part of our civil liberties and privacy depends on the social norms in technology industry and the design of software and computer architecture by engineers in the technology companies. To maintain the balance between privacy and governance in a digital age, we need a joint efforts from social, legal and technical aspects for a better cyberspace.

107 Monahan, "Questioning Surveillance and Security," 103.

Works Cited

Chesterman, Simon. *One Nation under Surveillance: A New Social Contract to Defend Freedom without Sacrificing Liberty*. Oxford: Oxford University Press, 2011.

Cohen, Joshua. "Privacy, Pluralism and Democracy." In *Philosophy, Politics, Democracy: Selected Essays*. Cambridge, Massachusetts: Harvard University Press, 2009.

Dewey, John. *Democracy and Education*. Champaign, Ill.: Project Gutenberg, 1916.

Electronic Frontier Foundation. "CALEA." Accessed April 4, 2015. https://www.eff.org/issues/calea.

Ellickson, Robert C. *Order Without Law: How Neighbours Settle Disputes.* Cambridge: Harvard University Press, 1991.

Foucault, Michel. *Discipline and Punish: The Birth of the Prison*. New York: Pantheon Books, 1977.

Haggerty, Kevin D., and Richard V. Ericson. "The Surveillant Assemblage." *British Journal of Sociology,* 51, no.4 (2000): 605-22.

Haggerty, Kevin D., and Minas Samatas, eds. *Surveillance and Democracy*. Abingdon, Oxon: Routledge, 2010.

Kerr, Orin S. "A User's Guide to the Stored Communication Act - and a Legislator's Guide to Amend It." *George Washington Law Review,* 72 (2004): 1701-41.

Levy, Steven. *Crypto: How the Code Rebels Beat the Government, Saving Privacy in the Digital Age*. New York: Viking, 2001.

Lessig, Lawrence. *Code*. Version 2.0. ed. New York: Basic Books, 2008.

Lyon, David. *The Electronic Eye: The Rise of Surveillance Society*. Minneapolis: University of Minnesota Press, 1994.

Marx, Gary T. "A Tack in the Shoe: Neutralizing and Resisting the New Surveillance." *Journal of Social Issues*: 369-90.

Monahan, Torin. "Questioning Surveillance and Security." In *Surveillance and Democracy*, edited by Kevin D. Haggerty and Minas Samatas. Abingdon, Oxon: Routledge, 2010.

Monahan, Torin. *Surveillance in the Time of Insecurity*. New Brunswick, N.J.: Rutgers University Press, 2010.

Richards, Neil. *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*. New

York: Oxford University Press, 2015.

Schwartz, Paul. "Privacy and Democracy in Cyberspace." *Vanderbilt Law Review* 52 (1999): 1609.

Stanford Law School Center for Internet and Society. "Big Data and Privacy: Making Ends Meet." *Society Future for Privacy Forum Essay Collection* (2013).

Solove, Daniel J. *Nothing to Hide: The False Tradeoff between Privacy and Security*. New Haven, Conn.: Yale University Press, 2011.

Solove, Daniel J. *The Digital Person: Technology and Privacy in the Information Age*. New York: New York University Press, 2004.

Solove, Daniel J. *Understanding Privacy*. Cambridge, Mass.: Harvard University Press, 2008.

Sotomayor, Sonia. United States v. Jones. 565 U.S. 10-1259 (2012) (Sotomayor, J., concurring).

Vagle, Jeffrey L. "Furtive Encryption: Power, Trust, and the Constitutional Cost of Collective Surveillance." *Indiana Law Journal* 90 (2015): 191-241